

Reconsideration of this application, as amended, is respectfully requested.

Objection to the Specification

The Examiner has objected to the title of the invention as being too generic.

In order to overcome this objection, Applicant has amended the title of the invention. Applicant has attempted to briefly indicate a feature of the present invention that distinguishes the database security system from other database security systems.

Accordingly, reconsideration and withdrawal of this objection are respectfully requested.

Rejection Under 35 U.S.C. § 103

Claims 1-2 and 5-8 stand rejected under 35 U.S.C. § 103 as being unpatentable over McDonnal et al. Claims 3-4 stand rejected under 35 U.S.C. § 103 as being unpatentable over McDonnal et al. and further in view of Applicant's admitted prior art. In the Interview Summary dated July 19, 2000, the Examiner indicates that claims 9-17 stand rejected under 35 U.S.C. § 103 as being unpatentable over McDonnal et al. These rejections are respectfully traversed.

Applicant respectfully submits that the present invention, as recited in independent claims 1, 8 and 9, is significantly

distinguished from the teachings of McDonnal et al. Independent claims 1, 8 and 9 have been amended so as to clearly set forth that the first database (O-DB) includes "a table structure with rows and columns, each row representing a record (P) and each combination of a row and a column representing a data element value (DV)." For illustration purposes, such an arrangement is depicted in Applicant's Figure 4, wherein it can be clearly seen that each record (P) comprises a plurality of data element values (DV).

The present invention relates to a database management system. A commercial database system, which is operated by a database management system, is often called a relational database. The operation and handling of such a database system differs significantly from the operation and handling of a file management system. Examples of database management systems are Oracle 8i from Oracle Corporation and MicroSoft SQL Server from MicroSoft Corporation. Each of these database management systems are, in turn, often run by a file management system of an operating system such as MS-DOS by MicroSoft Corporation or UNIX.

Both the syntax, and particularly the structuring of data, differ in a database management system versus a file management system. Another important difference is the integrity of the data structures. It is quite apparent from the language of independent claims 1, 8 and 9, that the present invention relates to a database

management system, especially when looking at the context of the terms used, such as record (P), data element value (DV), data element type (DT).

McDonnal et al. primarily focuses on the protection of files in a file system. In column 33, line 66 through column 34, line 8, McDonnal et al. does suggest that his routines could be used on a system with finer granularity than files, such as database records.

The present invention operates on an even finer granularity than taught by McDonnal et al. Namely, the present invention operates on the data element values (DV) level of granularity in the database management system. It is thus the individual data element (DV), and not the entire record (P), that becomes the controlling unit. For example, a person could be given access to a database with personal information, but only to read parts of the records (P), for example, age or sex, but not information about personal health.

Even if one of ordinary skill in the art had tried to apply the routines of McDonnal et al. to data element values in a database management system, one would not have given protection to the database records. First, if the routines would have been applicable, the routines would have left database values unencrypted in periods of time. Secondly, such routines would not have worked in such a fine granular environment.

The reason that McDonnal et al.'s routines would not have worked in such a fine granular environment is that a relational database contains tables with columns and rows. Each row represents a database record, and the columns contain the different data values of a record. It is not defined in McDonnal et al. where the encrypted data values would be temporarily stored under new names. It is not feasible to create temporary columns (data element values) during reading of the database. It is also not feasible to write the decrypted data back to the original data value, since there are restrictions on column values in database systems.

In view of these observations, it would not have been obvious to one of ordinary skill in the art to have modified the file management system of McDonnal et al. in order to arrive at a database management system operating on a data element value level, as set forth in Applicant's independent claims.

As further areas of distinction, McDonnal et al. describe a system for protecting files in a file management system by automatic encryption, decryption and re-encryption of files. In the system of McDonnal et al., hidden files (169) are preferably stored in the same file system, and more preferably in the same directory, as the files to be protected. These hidden files describe each file in the directory which is subject to encryption. When a user attempts to access a file using a program, the program sends an OPEN command to

the OS-Kernel. Then, the system of McDonnal et al., via a routine (200), intercepts this call for opening the file. The routine performs the following steps 233-243: saving the original name of the requested file (233); renaming the original requested file (234); opening the renamed original for reading (235); opening a new file with the original name of the original requested file (236); reading from the renamed original file (241); decrypting read data (242); and writing plaintext to the new file. Thus, at this point, there are two files in the file system having the same content, the original encrypted file with a new name and a new plaintext file with the original name.

Therefore, in the McDonnal et al. system, there exists a certain state in the system wherein there is a probability that files, defined to be protected in the hidden files (169), exists in plaintext form, because they are in use by a program. It is then possible for another user to scan the storage media where the files are stored, such as the hard disk, for the plaintext files in order to obtain decrypted sensitive data.

In the present invention, the data element values remain encrypted in the database during the processing of the data element. A data element value in the decrypted form exists only in the program accessing the data element value, the decrypted data element value is never stored. When a programmer is finished processing a

decrypted data element value, it is either erased from the computer's memory or the database is updated with a new encrypted data element value.

Because the combinations, as set forth in Applicant's claims, are not shown nor fairly suggested by the prior art of record, reconsideration and withdrawal of these rejections are respectfully requested.

CONCLUSION

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), the Applicant respectfully petitions for a one (1) month extension of time for filing a response in connection with the present application and the required fee of \$110.00 is attached hereto.

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn.

It is believed that a full and complete response has been made to the Office Action, and as such, the present application is in condition for allowance.

In the event there are any outstanding matters remaining in this application the Examiner is invited to contact Mr. Scott L.

Appl. No. 09/027,585

Lowe (Reg. No. 41,458) at (703) 205-8000 in the Washington, D.C. area to discuss these matters.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By Joe McKinney Muncy
Joe McKinney Muncy, #32,334

MM
KM/SLL/smm
0104-0221P

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000